2016 年物联网安全报告

杭州安恒信息技术有限公司

2016 年 10 月

目录（CONTENTS）

1. 物联网概述

物联网是新一代信息技术的重要组成部分，也是“信息化”时代的重要发展阶段。其英文名称是：“Internet of things（IoT）”。顾名思义，物联网就是物物相连的互联网，也是智能硬件的互联网。这有两层意思：其一，物联网的核心和基础仍然是互联网，是在互联网基础上的延伸和扩展的网络；其二，其用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通信，也就是物物相息。

2012 年 2 月 14 日，中国的第一个物联网五年规划——《物联网“十二五”发展规划》由工信部颁布。

物联网开始在各个行业大量应用，包括智能农业、智能电网、智能交通、智能物流、智能医疗、智能家居等等。全球市场数据统计分析显示，物联网将成为未来 10 年发展最迅速的行业之一，到 2020 年，世界上的物联网业务将远远超过人与人之间的通信业务，从这方面来看，物联网将会是一个重量级的信息技术方面的产业。

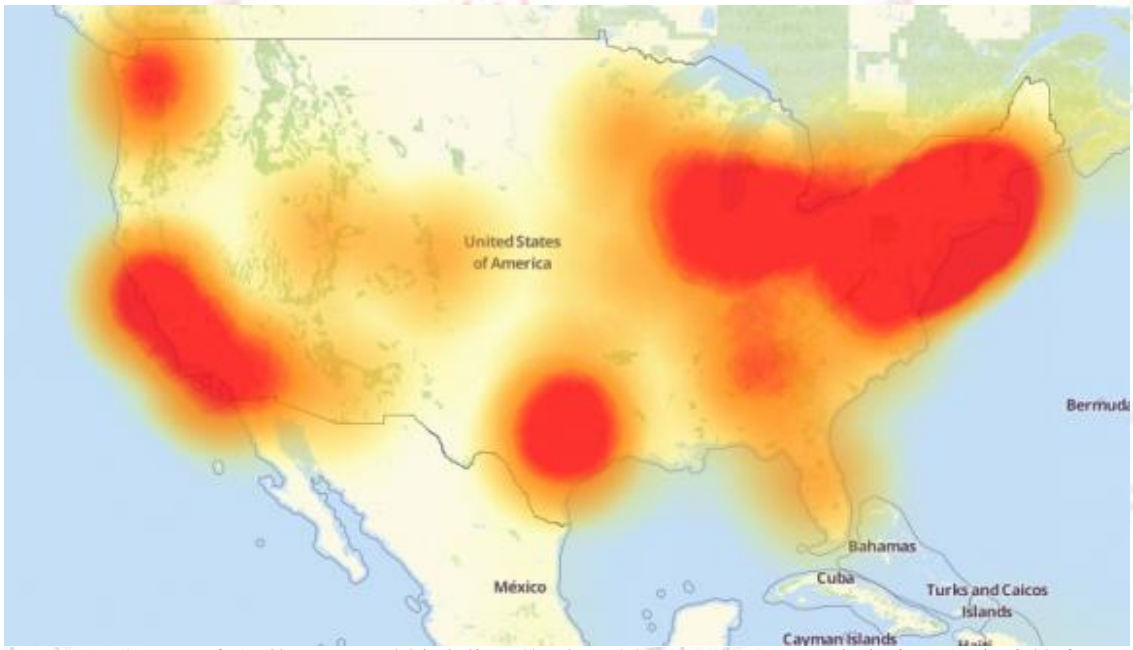
物联网的快速发展也带来一系列的安全问题，尤其是在线监控设备数量增长迅速，一方面可能会被黑客利用作为海量攻击来源，如物联网僵尸网络病毒“Mirai”在美国半个国家互联网瘫痪事件中扮演了重要角色，另外一方面，隐私泄漏、身份伪造、弱口令、漏洞利用等也是物联网自身面临的安全威胁。

2. 2016 年物联网安全事件

2.1. 美国半数互联网断网，智能监控设备为攻击源

2016 年 10 月 21 日，美国域名服务器管理服务供应商 Dyn 宣布，该公司在当地时间周五早上被 Mirai 僵尸网络（由被攻击的物联网设备组成，包括 DVR 和网络摄像头）发起大规模 DDoS 攻击。主要原因是黑客在 2016 年 10 月 21 日通过互联网控制了大量的网络摄像头和相关的 DVR 录像机，然后操纵这些「肉鸡」攻击了美国的多个知名网站，包括

Twitter、Paypal、Spotify 在内多个人们每天都用的网站被迫中断服务。美国主要公共服务、社交平台、民众网络服务瘫痪。



据了解，黑客们使用了一种被称作「物联网破坏者」的 Mirai 病毒来进行肉鸡搜索。更为致命的是，Mirai 病毒的源代码在 9 月的时候被开发者公布，致使大量黑客对这个病毒进行了升级，传染性、危害性比前代更高。Mirai 病毒是一种通过互联网搜索物联网设备的一种病毒，当它扫描到一个物联网设备（比如网络摄像头、智能开关等）后就尝试使用默认密码进行登陆（一般为 admin/admin，Mirai 病毒自带 60 个通用密码），一旦登陆成功，这台物联网设备就进入「肉鸡」名单，开始被黑客操控攻击其他网络设备。

因为传播范围广，给美国的互联网带去了严重的影响，超过半数人周五无法上网，美国国土安全部和联邦调查局都已经表示开始进行调查。

根据国外网站 KerbsonSecurity 的调查，导致大规模断网事件的原因绝非我们想象的那么简单，其背后暴露出物联网设备的重大安全隐患。

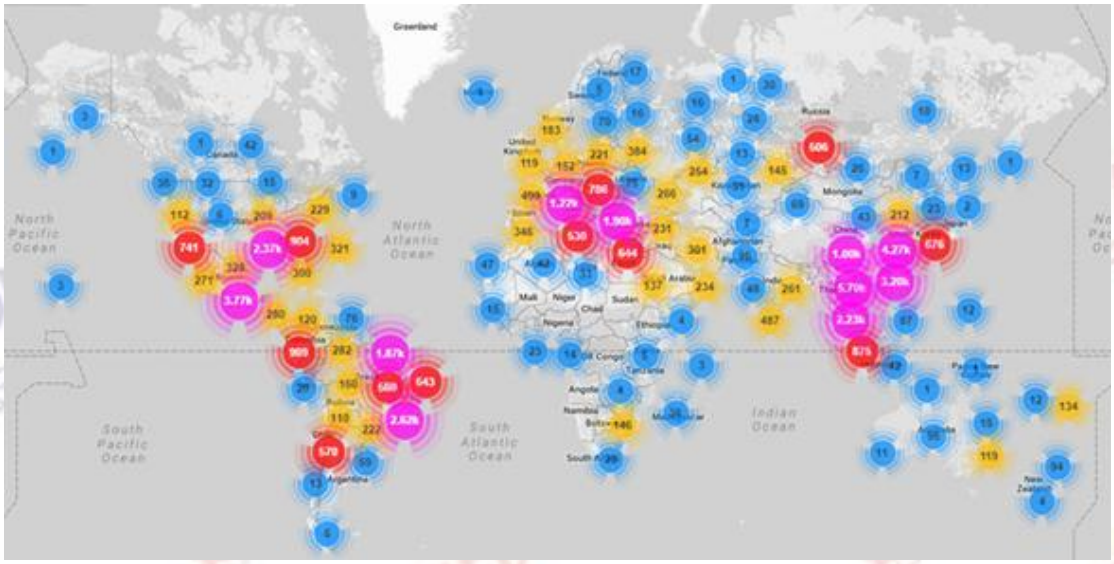
据报道，一共有超过百万台物联网设备参与了此次 DDoS 攻击。其中，这些设备中有大量的 DVR（数字录像机，一般用来记录监控录像，用户可联网查看）和网络摄像头（通过 Wifi 来联网，用户可以使用 App 进行实时查看的摄像头）。

由于监控设备模组中的密码被写入到了固件中，还没有工具可以修改这个模组的密码。更可怕的是，用户根本不知道还有这么一个密码的存在。跟雄迈科技相似的公司还有很多，他们也开发摄像模组，也研发 DVR 解决方案。

于是乎，在黑客套上通用的帐户名和密码之后，轻松地控制了这超过 100 万台设备，也导致了此次大规模 DDoS 攻击事件。据悉，目前还没有比较好的解决方案来解决这个问题，这些肉鸡只有被断网后才会停止攻击。

2.2. 全球 80%国家的物联网设备感染病毒“Mirai”

据国外安全公司统计，由受 Mirai 感染设备组成的僵尸网络已遍及 164 个国家。该公司研究人员“MalwareTech”还标记受 Mirai 感染的国家。据他统计，受影响的国家甚至高达 177 个。，约占全球国家的 80%。“Mirai”过去几年曾发起最大的 DoS 网络攻击。



2016 年 9 月 Mirai 还针对知名安全记者 Brian Krebs 博客网站发起大规模 DDoS 攻击。

2016 年 10 月，黑客公布了“Mirai”源代码，这样一来，便为技能较低的网络罪犯发动网络攻击提供新工具，也为互联网防御者及安全研究人员提供方法追踪黑客活动，并映射被入侵设备的网络。

Mirai 的确算不上一款特别的恶意软件，但却十分有效并能迅速传播，因为它的目标是极易入侵的物联网设备。这些设备大多为 DVR 和监控摄像机，并使用默认和极易预测的用户名和密码，比如“admin”和“123456”；“root”和“password”或“guest”和“guest”等。由于这些弱密码的存在，Mirai 恶意软件便能感染全球脆弱的物联网设备。

2.3. 物联网变种新威胁 Hajime 蠕虫更复杂

根据 Rapidity Networks 的安全研究人员 Sam Edwards 和 Ioannis Profetis 发现了 Hajime。是一款新型物联网蠕虫，其传播方式与 Mirai 一致，但 Hajime 通过蛮力攻击自行传播，它使用三级感染机制并自行传播。Stage 0 发生在已被感染的系统上，Hajime 从这里开始扫描随机 IPv4 地址。

Hajime 在端口 23 发起蛮力攻击，试图通过源代码中硬编的一系列用户和密码登录另一端。如果 IP 地址的端口 23 未打开，或蛮力攻击失败，Hajime 将移至新 IP。

如果连接成功，Hajime 将执行以下四个命令：

- enable
- system
- shell
- sh /bin/busybox ECCHI

这些命令允许该蠕虫告知其是否感染了 Linux 系统。Hajime 与其它物联网恶意软件类似，但却不同。Hajime 的操作方式比 Mirai 更胜一筹，似乎还借鉴了许多其它物联网恶意软件的技巧。Hajime 使用 DHT 连接到 P2P 僵尸网络，跟 Rex 类似；使用内置的用户名和密码列表蛮力攻击随机 IP 并自行传播。

Hajime 还能攻击以下平台：ARMv5、ARMv7、Intel x86-64、MIPS 和 little-endian。不同点在于 Hajime 用 C 语言编写，而不是 Go（Rex）；使用的是 P2P 网络，而不是直接 C&C 服务器连接（Mirai）；能在大量平台运作，也不仅仅是 MIPS（NyaDrop）。因此，Hajime 似乎吸纳其它物联网恶意软件的优点，比今天我们看到的物联网恶意软件复杂得多。

Hajime 以网络摄像机、DVR 和 CCTV 系统为目标。更具体而言，其目标设备由 Dahua Technologies（大华技术）、ZTE（中兴）以及购买 XiongMai Technologies（雄迈科技）白色标签 DVR 系统的其它公司生产制造。

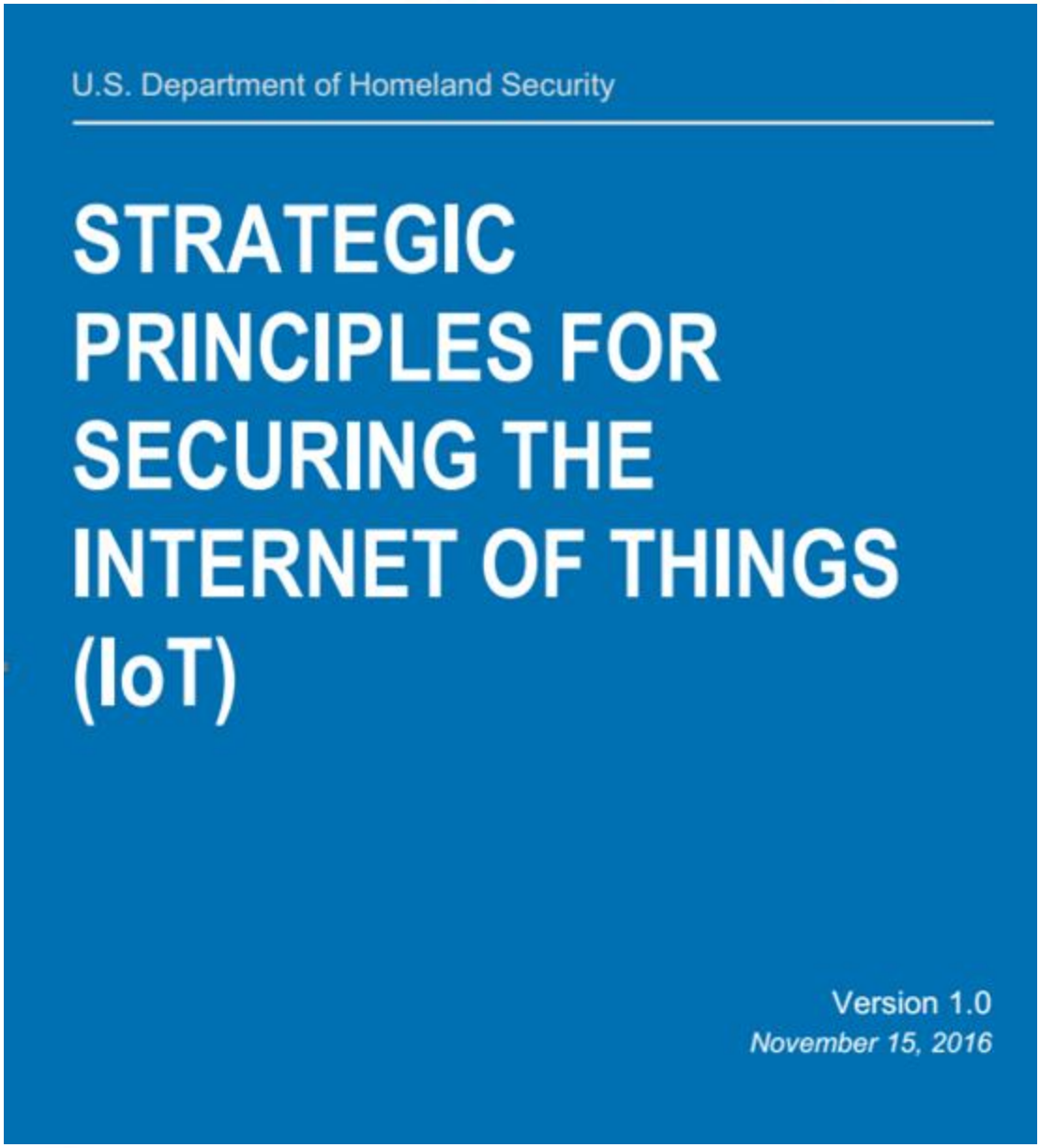
对于 Hajime 的幕后黑手，Rapidity 研究人员表示：“文件时间戳经分析后表明，该蠕虫开发人员在协调世界时 UTC 15:00-23:00 最为活跃，UTC 00:00-05:00 停止活动。这个时间大致符合欧洲的睡眠模式。”

3. 国际物联网安全动态

3.1. 美国 DHS 发布《保障物联网安全战略原则》

2016 年 11 月 15 日，美国国土安全部（DHS）发布“保障物联网安全的战略原则 v1.0”，要求物联网制造商必须在产品设计阶段构建安全，否则可能会被起诉。

该战略原则指出，未在最初设计阶段构建安全并采取基本安全措施“可能会造成制造商的经济成本、声誉成本或产品召回成本损失。虽然还没有建立解决物联网问题的判例法体系，但传统的产品责任侵权原则可以适用。”



以下为简单概括部分物联网安全高级原则：

·在设计阶段结合安全：“经济驱动力使得企业将设备推入市场时很少考虑安全。这给恶意攻击者创造大量机会操控联网设备的信息流”。

·启用安全更新和漏洞管理：即使安全从一开就内置存在，但在产品部署后发现产品漏洞很常见。这些漏洞能通过补丁、安全更新和漏洞管理策略缓解。

·**建立在可靠的安全最佳实践之上：**传统网络安全中许多经过验证的实践可以作为提升物联网安全的出发点。

·**根据影响优先考虑安全措施：**数据泄露的风险和后果大不相同，这取决于联网设备。因此，专注破坏、泄露或恶意活动的潜在后果对决定物联网生态系统的安全方向尤为重要。

·**提升透明度：**在可能的情况下，开发人员和制造商需要了解供应链，因此他们能识别软件和硬件组件，并了解任何相关漏洞。增强意识能帮助制造商和工业消费者识别安全措施应用的位置和具体方法。

·**连接需仔细谨慎：**考虑物联网的使用和物联网被破坏的相关风险，物联网消费者，尤其工业企业应该仔细并谨慎考虑是否需持续连网。

西尔维斯表示，“今天迈出了第一步”。他承认，联邦机构、行业组织等在不懈努力。战略原则指出，物联网存在的许多漏洞能通过公认的安全最佳实践得到缓解，但如今太多产品未融入最基本的安全措施。

在此战略原则中，DHS 定义了联邦机构需要执行的四项物联网安全事项：

·**协调**其它联邦部门和机构与物联网制造商、网络连接提供商和其它行业利益相关者合作。随着进一步细化和理解最佳实践和方法，未来的努力方向还将集中在更新和应用这些原则上。

·在所有利益相关者中构建与物联网有关的**风险意识**。DHS 将与其它机构、私有部门和国际合作伙伴合作增强公众意识、教育和培训计划。

·**识别并推进激励措施，**保障物联网设备和网络安全。现在，常常搞不清楚谁是给定产品或系统的安全负责人。此外，安全性差所带来的成本通常不由增强安全的人承担。要考

虑的因素是侵权责任、网络保险、立法、监管、自愿认证管理、标准设定举措、自愿行业级计划…今后，DHS 将召集合作伙伴讨论这些重大事项、并收集意见和反馈。

·**为物联网国际标准发展进程做贡献**。美国的物联网设备是全球生态系统的一部分，更不用说国家组织正在全力应对同样的安全问题，开始评估众多同样的安全考虑。我们必须与国际合作伙伴和私营部门合作，支持国家标准的发展。该原则指出，重要的是，不将物联网的相关活动分裂为不一致的标准或规则集。

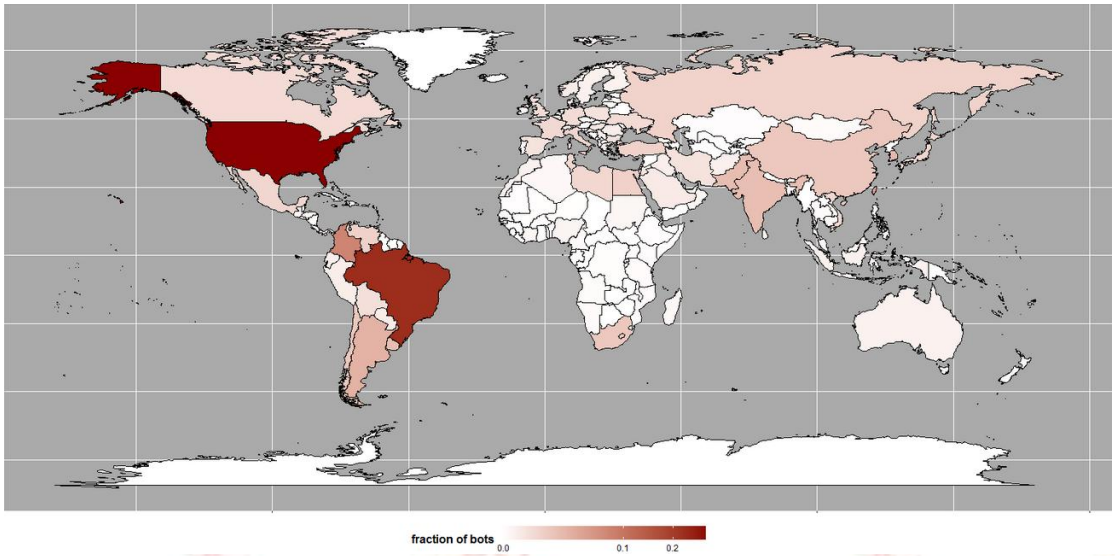
根据战略原则总结："美国无法承担不安全物联网设备带来的影响。考虑到对关键基础设施、个人隐私和经济的潜在损害，后果不堪重负"。

3.2. 全球 80%被病毒感染物联网设备为监控设备

Mirai 软件开发人员声称，Mirai 恶意代码感染了超过 38 万物联网设备，但这只是源代码公开前的数据。自从 Mirai 恶意软件开发人员在网上公布源代码后，物联网设备就成为易受恶意软件感染的高危受害者。

2016 年 10 月，当 Mirai 源代码公开后，美国 Level3 Communications 研究小组根据对 Mirai 的活动监视情况，他们得出结论：自从源代码公开后，被感染的物联网设备数量翻倍。研究小组监控了 Mirai 的命令与控制服务器，并确定约有 50 万台物联网设备被感染。但这只是起初的数据，实际数据可能更高。原因就在于，源代码公开后，数个新僵尸网络如雨后春笋般萌芽，导致大量设备被感染。

该研究小组还发现，近 10 万 bots 用于 DDoS 攻击监视针对一个目标。其中超过 80%的 bots 实际上是 DVR。Mirai 恶意软件能识别并感染大范围的物联网设备，包括 Linux 服务器、路由器、网络摄像头和 Sierra 无线网关。其中至少四分之一的被感染设备在美国，其后是巴西，占比 23%，哥伦比亚占比 8%。



其中超过四分之一 Mirai bots 包含另一个强大恶意软件 Lizkebab 或 Bashlite。这就意味着，多种恶意软件以某个特定设备为目标。让人惊讶的是，使用 Bashlite bots 发起 DDoS 攻击期间，Mirai 的命令与控制服务器数次成为目标。

3.3. 全球数百万物联网设备暴露在互联网

美国的 SEC consult 分析了来自 70 多家厂商的超过 4000 个固件的嵌入式设备。发现许多这些设备在互联网上都可以通过不安全的配置直接访问，比如 Ubiquiti Networks 公司——在默认的况下把大多数的产品都启用了远程管理。

Seagate（希捷）GoFlex 的许多（80.000 个）都暴露了 HTTPS 和 SSH，这应该怪希捷通过 UPnP 设置端口转发分享了功能。

互联网服务供应商包括 CenturyLink（500,000 个被曝光的设备），TELMEX（1 亿台设备），Telefonica（170,000 设 备），中国电信（100,000 个设备），VTR Globalcom（55,000 个设备），Chunghwa Telecom（45,000 个设备）和 Telstra（26000 个设备），这些公司的调制解调器，路由器和网关等设备的 HTTPS 和 SSH 远程管理功能在默认情况下是启用的。

根据 SEC consult 总结的数据显示，最受影响的主机所在国家是：

1	United States	26,27%
2	Mexico	16,52%
3	Brazil	8,10%
4	Spain	5,60%
5	Colombia	4,36%
6	Canada	3,25%
7	China	3,20%
8	Russian Federation	2,36%

从 50 个有问题的厂商中发现了超过 900 个产品，名单如下：

ADB, AMX, Actiontec, Adtran, Alcatel-Lucent, Alpha Networks, Aruba Networks, Aztech, Bewan, Busch-Jaeger, CTC Union, Cisco, Clear, Comtrend, D-Link, Deutsche Telekom, DrayTek, Edimax, General Electric (GE), Green Packet, Huawei, Infomark, Innatech, Linksys, Motorola, Moxa, NETGEAR, NetComm Wireless, ONT, Observa Telecom, Opengear, Pace, Philips, Pirelli , Robustel, Sagemcom, Seagate, Seowon Intech, Sierra Wireless, Smart RG, TP-LINK, TRENDnet, Technicolor, Tenda, Totolink, unify, UPVEL, Ubee Interactive, Ubiquiti Networks, Vodafone, Western Digital, ZTE, Zhone 和 ZyXEL。

3.4. 全球超过四分之一的物联网设备存在弱口令

2016 年 12 月，根据安恒海特实验室对全球主流监控设备的分布进行分析，发现在全球公网中暴露出来的国内主流监控设备数量已经达到数百万台，其中存在有弱口令的设备已探测达到 27%。依据上述数据，可分析得知大约超过四分之一的暴露物联网设备可能存在安全问题。

另外，据美国 SEC consult 对互联网网关，路由器，调制解调器，IP 摄像头，VoIP 电话等物联网设备分析的结果显示，在大概 4000 个固件中发现了大约有 580 个特别的私钥，其中有 230 个密钥被经常重复使用：

- “网络上超过 9%的 HTTPS 主机的私钥（大约 150 个服务器证书，被 320 万台主机使用着）”
- “网络上超过 6%的 SSH 主机的私钥（大约 80 个 SSH 主机密钥，被 0.9 万台主机使用着）”

物联网设备上运行的固件的嵌入式密钥主要用于 HTTPS 和 SSH 连接，这种做法很有风险，会将最终的用户暴露在攻击者面前。攻击者可以很容易地找到密钥，从而进入数量惊人的共享物联网设备中。

4. 物联网安全威胁

4.1. 智能家居安全威胁

智能家居已经进入了我们生活的方方面面，但智能设备在带来便利的同时也带来了安全风险。TrapX Security 的研究者发现联网状态下的 Nest（谷歌收购的智能家居公司）温度调节器存在漏洞，可以通过入侵温度调节器进一步入侵同一网络下的其他设备。

主要是通过设备的 USB 端口入侵 Linux 操作系统便可掌控温度调节器。并把自定义的恶意软件加载到温度调节器上，阻止用户的温度调节器数据发送回 Nest 服务器。同样的方法，可以在 RAM7 处理器芯片上加载恶意软件。可以随意查看到很多温度调节器上的数据，包括本地网络的无线密码和同一网络下其他用户的有关数据。

研究人员发现，存储在 Nest 本地的数据没有加密，但是在通过云传输发送数据到服务器时却使用了加密。在测试中，研究者可通过利用设备上存在的已知漏洞获得设备的管理员权限，然后还可入侵同一网络下的其他设备。

4.2. 智能电视安全威胁

从智能电视开始越来越多使用，也出现更多安全方面的问题，尤其是在用户使用过程中对用户隐私和正常使用方面的影响，已经危害到正常的使用和生活，因此智能电视的安全威胁亟待重视和加强。

2016 年 12 月，美国一名居民由于想看电影而下载了一款包含勒索程序的软件，在开机的时候会显示虚假的 FBI 警告，要求感染者在三天内支付 500 美元的罚款。受感染的是一台 3 年前出厂的 LG 电视（型号为 50GA6400）。用户随后联系 LG 方面经过多次沟通，他的电视才得到了修复。

美国安全供应商 Sucuri 对 2016 年上半年极度活跃的僵尸网络进行调查，发现这些僵尸网络是 DDoS 攻击的核心，经过对 DDOS 攻击的来源进行调查，发现攻击来自超过 25,513 个唯一 IP 地址，一些为 IPv6 地址。这些 IP 地址经确认都是来自闭路电视系统。其中中国台湾地区占了所有 IP 的约四分之一。

4.3. 智能汽车安全威胁

在物联网的广阔领域中，车联网是增速最快的细分市场之一。2013 年 6 月，WiFi 联盟宣布正式发布 IEEE 802.11ac 无线标准认证，标志着 5G Wi-Fi 时代的来临。

但日益复杂的高科技汽车今后也将越来越容易受到黑客的攻击，他们会借助智能汽车无线连接访问个人信息。而更令人担忧的是，在急于在车辆当中安装这些高科技的汽车制造商可能不知道这些危险，因此也就没有采取严格的安全措施。

车联网的通信网络有三大挑战：攻点多、传播快、评测难。从云平台角度来说，因为大量的车辆运行有大量的数据后台管理，这里面临着数据量大、实施服务、数据质量不稳定和软件演化导致的一系列挑战。

根据安恒海特实验室的研究，安全研究员可以轻松利用奥迪，马自达，现代，丰田等汽车的漏洞，在智能汽车熄火锁车之后，利用重放攻击，可以实现快速解锁并启动汽车，进而对汽车进行任何想要的操控。

美国 Ed Markey 分别向 BMW、克莱斯勒、福特、通用、本田、现代、捷豹路虎、马自达、梅赛德斯-奔驰、三菱、 日产、保时捷、斯巴鲁、丰田、大众（奥迪）和沃尔沃等 20 家汽车制造商发函询问它们是否清楚和采用了汽车智能系统安全措施同时给予足够的重视，结果是很多厂商给出的安全措施并不足够，有些厂商甚至不知道黑客攻击会造成的危害。也有报告指出现代汽车所使用的新技术可以搜集用户的个人数据，包括了驾驶习惯和位置等。

4.4. 监控设备安全威胁

新型智能监控设备通常具有独立的操作系统，互联网不会将其视为特定设备，而是认为其属于完整的计算机，运行有最新的 Windows 或者 Linux 软件，拥有丰富的内存与强大的供电电源，同时亦接入快速互联网链接。黑客正是利用这样的认知不对称性实现设备控制，并最终致使互联网陷入崩溃——而作为安全从业者，我们对此完全无能为力。

2016 年 12 月，根据安恒海特实验室对全球主流监控设备在分布进行分析，发现在全球公网中暴露出来的国内主流监控设备数量已经达到数百万台，其中存在有弱口令的设备已探测达到 27%。依据上述数据，可分析得知大约超过四分之一的暴露物联网设备可能存在安全问题。

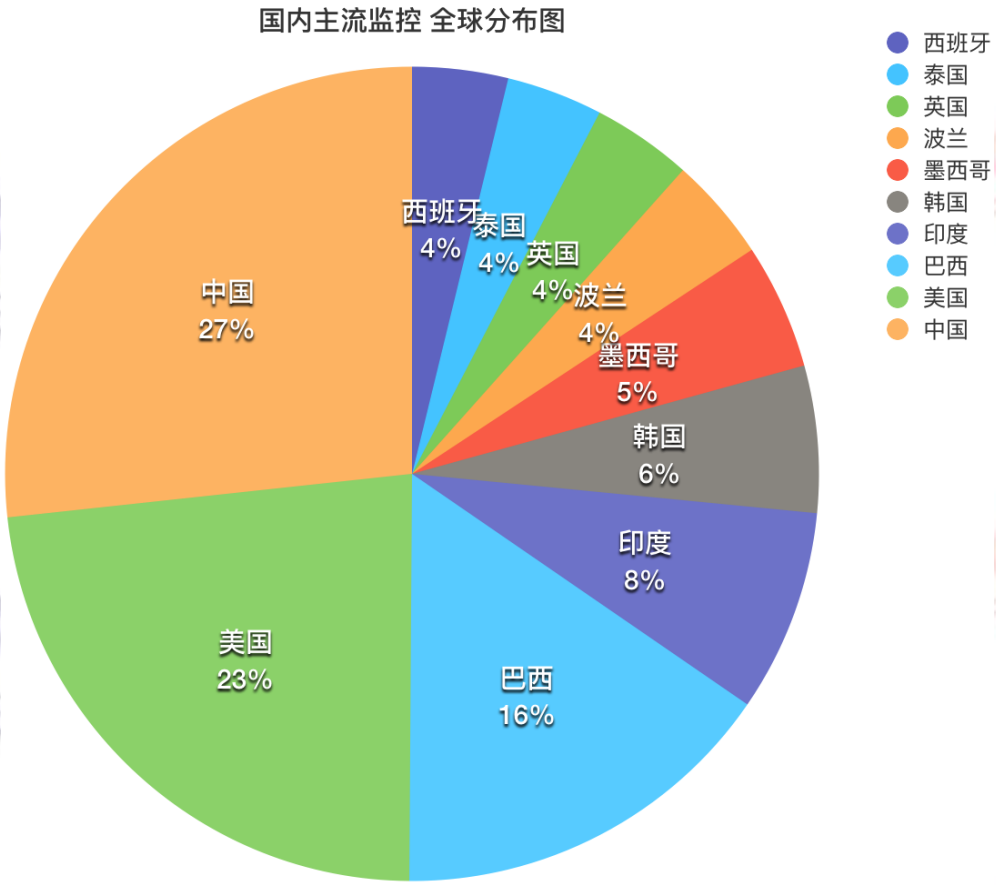
2016 年，安全公司 Protection1 也对监控设备发布了安全研究报告，指出美国境内有超过 6000 台无密码、开放访问的安全摄像头。这些安全摄像头都位于公共场所、私人企业的总部甚至是很多美国人的家庭中。

由于监控设备的特殊性导致,攻击者可以通过对批量监控设备的入侵来监控某个地区，导致攻击者可长期了解熟悉监控区域的活动情况。

5. 全球监控设备安全分析

5.1. 监控设备全球分布

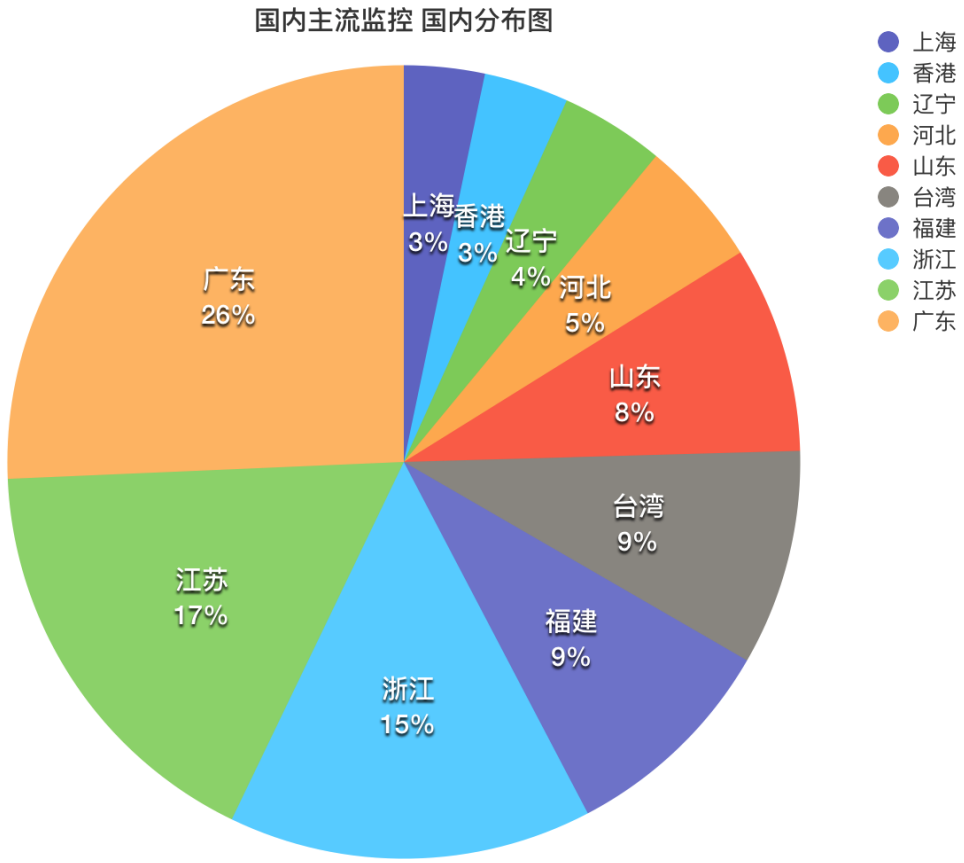
根据安恒海特实验室对监控设备进行安全监测的结果，可以得出暴露在公网的国家分布图，从图中我们可以看到中国占据第一位,美国第二位,巴西第三位，根据统计数据发现中国暴露出来的设备数量更多一些。



区域	数量
中国	470406
美国	408262
巴西	273440
印度	141592
韩国	102676
墨西哥	87829
波兰	72733
英国	69924
泰国	67340
西班牙	66966

5.2. 监控设备境内分布

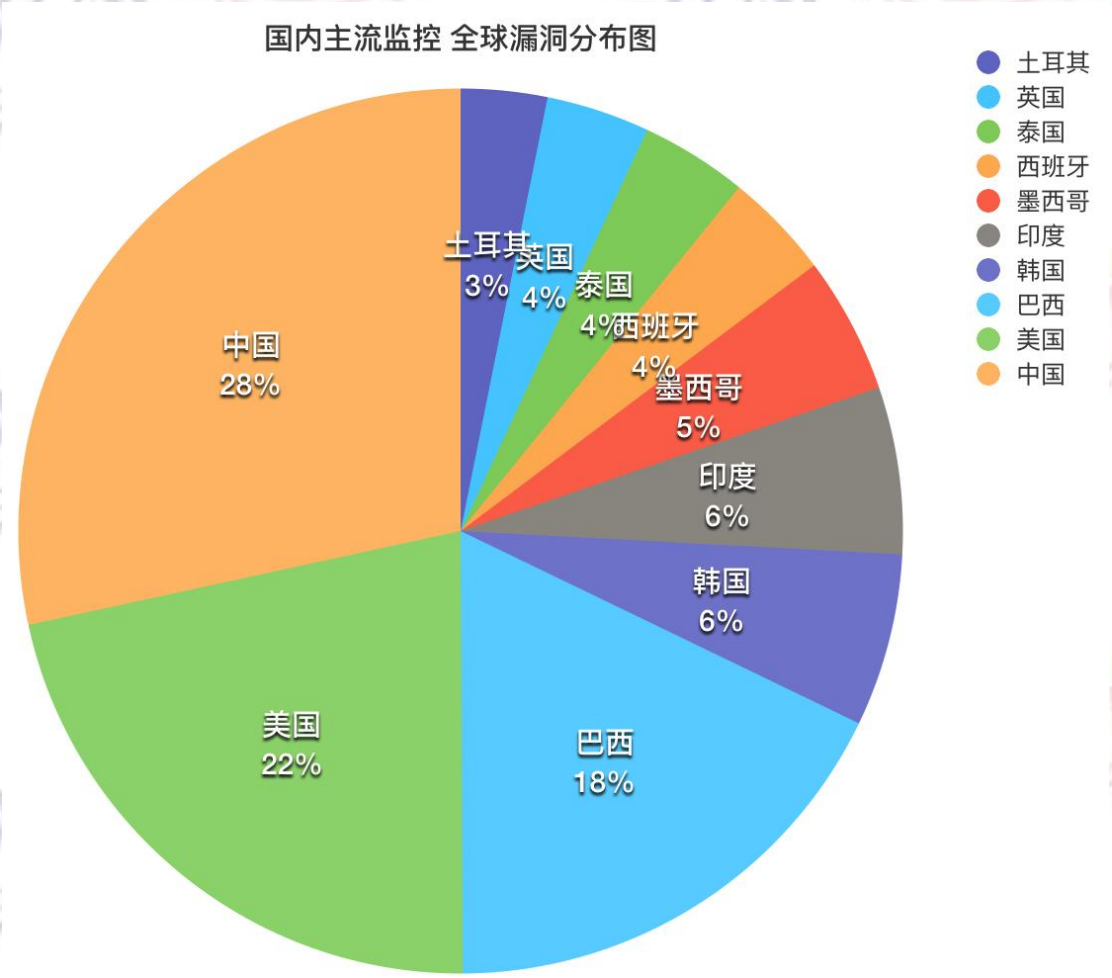
根据探测和发现，监控设备在国内省市的分布情况广东直接暴露在公网的监控设备相比其他省市暴露出来的更多，存在的安全风险也越高。



区域	数量
广东	89253
江苏	59685
浙江	51540
福建	31198
台湾	30535
山东	29223
河北	17946
辽宁	14729
香港	12028
上海	11409

5.3. 全球监控设备漏洞分布

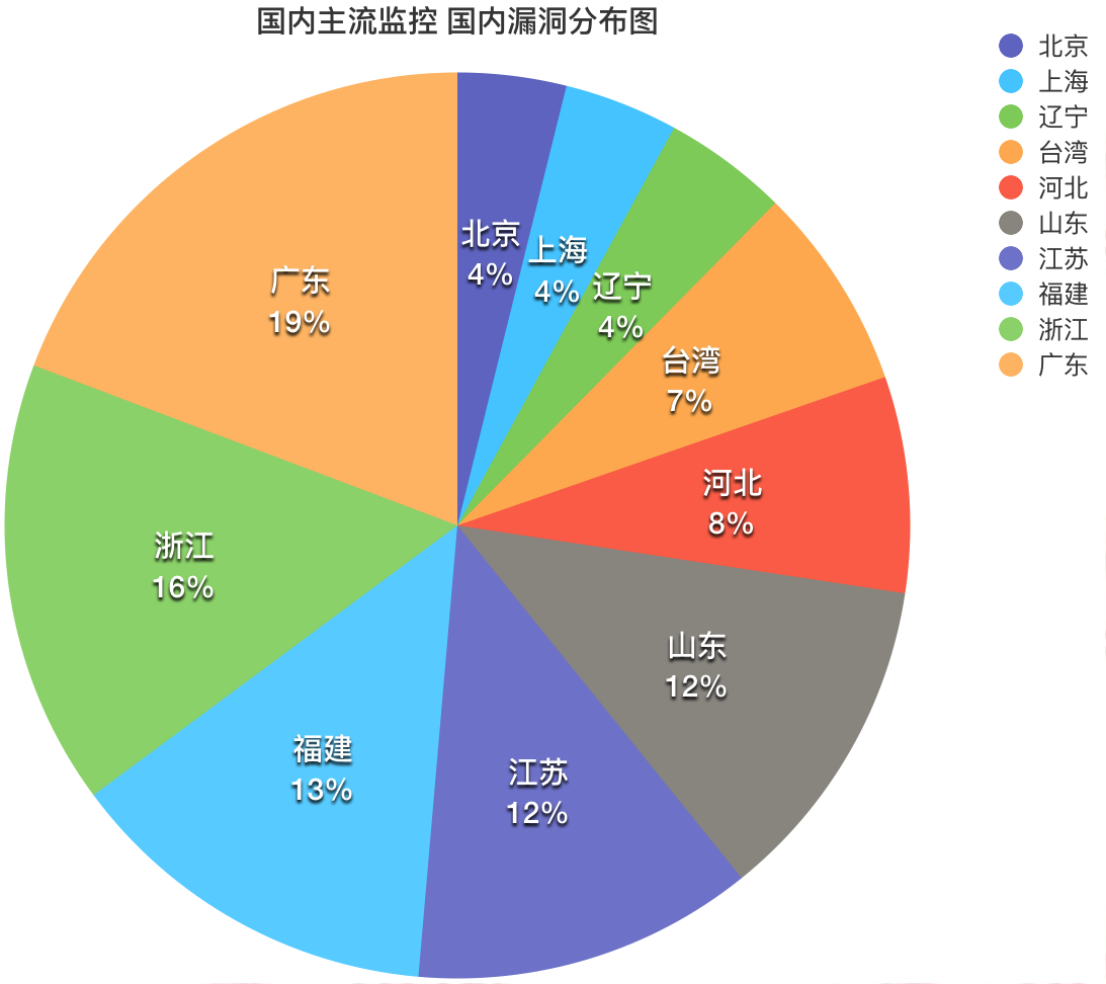
根据安恒海特实验室对监控设备进行安全监测的结果，中国存在漏洞的情况相比美国，巴西等地区更为严重，占比达到 28%。



区域	数量
中国	147850
美国	112824
巴西	92453
韩国	32878
印度	31748
墨西哥	25977
西班牙	20344
泰国	20337
英国	19681
土耳其	16408

5.4. 境内监控设备漏洞分布

根据安恒海特实验室对监控设备进行安全监测的结果，我们得知在国内省市内发现广东省漏洞数量多过其他区域。



区域	数量
广东	20743
浙江	17125
福建	14522
江苏	13114
山东	12716
河北	8309
台湾	7856
辽宁	4793
上海	4387
北京	4172

5.5. 全球监控设备漏洞占比

根据对监控设备的全球漏洞百分比分析，发现中国的监控设备数量和漏洞数量都非常高，其中存在漏洞的比例达到了 31.4%，位居第一位。

国内主流监控 全球范围内漏洞比

区域	设备数量	漏洞数量	漏洞比例
中国	470406	147850	31.4303%
美国	408262	112824	27.6352%
巴西	273440	92453	33.8111%
印度	141592	31748	22.4222%
韩国	102676	32878	32.0211%
墨西哥	87829	25977	29.5768%
波兰	72733	11663	16.0354%
英国	69924	19681	28.1463%
泰国	67340	20337	30.2005%
西班牙	66966	20344	30.3796%

根据监控设备国内漏洞数量百分比，中国的漏洞比大约 31%说明每 100 台设备中就有大约 31 台存在安全问题。

5.6. 境内监控设备漏洞占比

通过分析得知在福建地区存在的漏洞比例情况最为严重达到 46%，也说明大约每 100 台设备中就有 46 台存在安全问题。

国内主流监控 中国范围内漏洞比

区域	设备数量	漏洞数量	漏洞比例
广东	89253	20743	23.2407%
江苏	59685	13114	21.9720%
浙江	51540	17125	33.2266%
福建	31198	14522	46.5479%
台湾	30535	7856	25.7279%
山东	29223	12716	43.5137%
河北	17946	8309	46.3000%
辽宁	14729	4793	32.5412%
香港	12028	3887	32.3163%
上海	11409	4387	38.4521%

6. 物联网主要安全风险分析

物联网的核心技术通常有以下几个特点：可跟踪、可监控、可连接，尤其是监控设备、在线物联网设备等智能设备，这决定了其特点通常有分散化、规模庞大、边界模糊等方面，极易受到黑客攻击和利用，因此，其在安全方面的风险主要集中在以下几点：

6.1. 运行状态异常

物联网的设备通常数量非常庞大，同时部署位置也很分散化，可能会有断网、设备故障、状态异常等情况，因此，需要实时的对这些物联网设备状态进行实时的监控，及时发现异常的设备并进行预警。

6.2. 系统漏洞

物联网的设备通常都已经智能化，这些设备大多都有自己的操作系统，可能会存在系统漏洞未修复的情况。因此，需要实时的监测这些未修复的漏洞，并进行及时修复。

6.3. 系统弱口令

智能硬件的设备往往疏于管理，可能存在弱口令等问题，一旦被黑客利用后果极为严重，比如 2016 年下半年导致半个美国互联网瘫痪的 DDOS 攻击事件，其主要原因就是大量弱口令的智能硬件设备被黑客控制利用，因此，需要实时的监控系统存在的弱口令，并对其中存在问题的设备进行强化。

6.4. 身份伪造

智能硬件的设备可能部署在室外，会被恶意攻击利用，遭到替换设备并伪造身份，被利用作为攻击源，进而对整体物联网造成安全威胁。

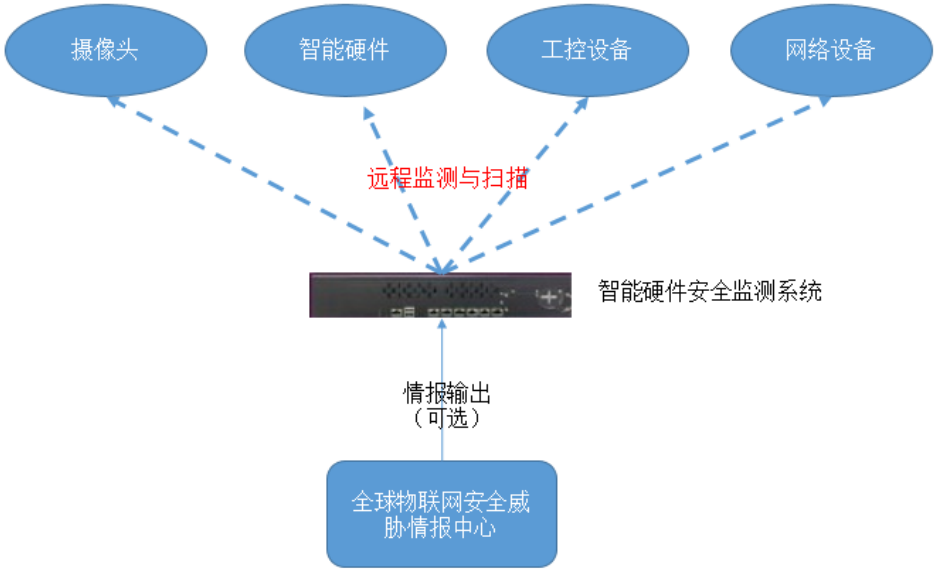
6.5. 非法接入

智能硬件物联网的设备类型多样，需要对这些设备进行及时的监控，发现其中仿冒的或非法的物联网设备类型。

7. 物联网安全监测技术方案

智能硬件物联网安全监测产品是安恒基于多年在应用安全、工控安全、云和大数据安全方面的积累，专门针对物联网安全需求研发，该产品部署灵活、安全监测能力强、实时性高，可以实时的监控智能硬件物联网设备的安全状况。

智能硬件物联网安全监测产品部署简单灵活，无需在各个区域独立部署，只需在监管中心部署即可实现对监管区域远程全覆盖监测，可以快速识别异常的智能硬件系统，发现智能硬件系统漏洞、弱口令等关键安全问题。



智能硬件物联网安全监测产品采用创新的技术手段，实现快速的对智能硬件设备如智能摄像头、智能工控设备等的安全监测与状态监测，及时发现其中的非法接入、异常伪造等问题。其具有以下技术特点：

7.1. 实时智能硬件状态监控

物联网安全监测产品采用创新引擎系统，可以实现每秒十万个物联网设备的快速监测与扫描，通过低间隔的轮询探测技术，可以实时的监控物联网设备安全状态，及时发现其中的在线、离线、故障等状态异常情况。

7.2. 快速智能硬件安全监测

物联网安全检测产品具备全面的漏洞检测能力，可以快速对硬件安全情况进行监测，实时发现其中系统漏洞、弱口令等情况。

7.3. 及时发现异常身份伪造

物联网安全检测产品可以快速扫描全网的物联网设备硬件信息，并形成硬件信息库，一旦发现其中身份仿冒、非法接入等情况，可以快速进行预警。

7.4. 实现在线设备指纹监测

物联网安全检测产品可以对所有在线设备进行深度的监测，发现其中的指纹信息，比如采用的硬件厂商类型、系统版本等信息，以便在发现 0day 漏洞情况下，快速的对相关设备进行预警。

7.5. 共享全球物联网安全威胁情报

物联网安全检测产品可以实时对接安恒全球物联网安全威胁情报中心，实时的更新最新的漏洞、策略库等情报信息，实现物联网安全威胁情报数据同步。